In the Claims:

1. (original) A document which comprises the name of an ostensible beneficiary in human readable form, together with machine readable encoded data that can be decoded to generate a unique identifier, the unique identifier being a function of unique data present in a human readable form on an identification item carried by a true beneficiary of the document, but having no simple functional relationship to any data on the document, such that the ostensible beneficiary of a document can be authenticated by comparing the unique identifier obtained from the document with the unique data on the identification item provided by the ostensible beneficiary.

2. (original) The document of Claim1 in which the document is a cheque and the ostensible beneficiary is the payee named on the cheque.

3. (currently amended) The document of Claim 1 ~~or 2~~ in which the machine readable encoded data is printed onto the document as a 1 or 2D bar code or other form of graphical symbology.

4. (original) The document of Claim 3 in which the machine readable encoded data can be scanned by a bar code scanner.

5. (original) The document of Claim 1 in which the document is selected from the following list of document types:
   (a) prescription for medicine;
   (b) tickets
   (c) tickets, stamps or other indicia issued by a third party to an end-user and printed by that end-user
   (d) credit, charge or debit card.

6. (original) The document of Claim 1 in which the identification item is selected from the following list of document types:

(a) identification card or other form of document
(b) passport
(c) drivers license
(d) document printed with biometric data
(e) iris
(f) finger

7. (original) The document of Claim 1 in which the identification item comprises a photographic image of the true beneficiary.

8. (original) The document of Claim 1 in which the machine readable encoded data is related to the unique data by a one way hash function.

9. (original) The document of Claim 1 in which the machine readable encoded data does not always appear in the same format in different documents associated with the same beneficiary.

10. (original) A method of authenticating an ostensible beneficiary presenting a document, in which the document comprises the name of the ostensible beneficiary in human readable form, together with machine readable encoded data that can be decoded to generate a unique identifier, the unique identifier also being a function of unique data present in a human readable form on an identification item carried by a true beneficiary of the document, but having no simple functional relationship to any data on the document, comprising the step of:

comparing the unique identifier obtained from the document with the unique data on the identification item provided by the ostensible beneficiary.

11. (original) The method of Claim 10 in which the document is a cheque and the ostensible beneficiary is the payee named on the cheque.

12. (original) The method of Claim 10 in which the machine readable encoded data is printed onto the document as a 1 or 2D bar code or other form of graphical symbology.

13. (original) The method of Claim 12 in which the machine readable encoded data can be scanned by a bar code scanner.

14. (original) The method of Claim 10 in which the document is selected from the following list of document types:
    (a) prescription for medicine;
    (b) tickets
    (c) tickets, stamps or other indicia issued by a third party to an end-user and printed by that end-user;
    (d) credit, charge or debit card.

15. (original) The method of Claim 10 in which the identification item is selected from the following list of document types:
    (a) identification card or other form of document
    (b) passport
    (c) drivers license
    (d) document printed with biometric data
    (e) iris
    (f) finger

16. (original) The method of Claim 10 in which the identification item comprises a photographic image of the true beneficiary.

17. (original) The method of Claim 10 in which the machine readable encoded data is related to the unique data by a one way hash function.

18. (original) The method of Claim 10 in which the machine readable encoded data does not always appear in the same format in different documents associated with the same beneficiary.